AO 106A (08/18) Application for a Warrant by Telephone or Other Reliable Electronic Means

UNITED STATES DISTRICT COURT

FILED
WILKES BARRE
SEP 20 2023
PER MS
DEPUTY CLERK

for the

Middle District of Pennsylvania

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

THE CONTENTS OF A 2005 TOYOTA SIENNA, TEXAS LICENSE PLATE: TCV6966 AND VIN: 5TDZA22C25S234412

Case No. 3:23-MC- 766

APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location):*

See Attachment "A"

located in the Middle District of Pennsylvania, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment "B"

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☑ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. §1029(a)(3) & (b)	Possession of 15 or more access devices & conspiracy to commit the same
18 U.S.C. §1029(a)(2) & (b)8	Use/trafficking in unauthorized access devices & conspiracy to commit the same
18 U.S.C. §1343	Wire fraud

The application is based on these facts:

See Affidavit of Probable Cause.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days *(give exact ending date if more than 30 days:* _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

F. Xavier Deluke
Applicant's signature

F. Xavier Deluke, FBI Special Agent
Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by Telephone *(specify reliable electronic means).*

Date: Sept. 20, 2023

Joseph F. Saporito, Jr.
Judge's signature

City and state: Wilkes-Barre, PA

Joseph F. Saporito, Jr., U.S. Magistrate Judge
Printed name and title

UNITED STATES DISTRICT COURT
MIDDLE DISTRICT OF PENNSYLVANIA

IN THE MATTER OF THE APPLICATION OF THE UNITED STATES FOR AUTHORIZATION TO SEARCH THE CONTENTS OF A 2005 TOYOTA SIENNA, TEXAS LICENSE PLATE: TCV6966 AND VIN: 5TDZA22C25S234412	**No.** 3:23MC766 **Filed Under Seal**

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Special Agent F. Xavier DeLuke, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. As a federal agent, I am authorized to investigate violations of United States laws and to execute warrants issued under the authority of the United States. I am an investigative or law enforcement officer of the United States within the meaning of 18 U.S.C. § 2510(7) and am empowered by 18 U.S.C § 3052 to conduct investigations of, and to make arrests for, violations of federal criminal statutes. I have been employed as a Special Agent with the Federal Bureau of Investigation (FBI) since December of 2021.

2. This affidavit is submitted in support of an application for a warrant to search the following item.

(a) A 2005 Toyota Sienna, blue in color having Texas license plate number TCV6966 and vehicle identification number 5TDZA22C25S234412 (VEHICLE TO BE SEARCHED) which was used to commit violations of Title 18, U.S.C. §§ 1029(a)(3) and (b), 1029(a)(2) and (b), 1343, and 1349. The aforementioned items are described in Attachment A, and the evidence to be searched and seized is described in Attachment B.

3. The facts set forth in this Affidavit come from my personal observations, my training and experience, evidence gathered during the investigation and information obtained from other law enforcement agents and witnesses. Because this Affidavit is submitted for the limited purpose of establishing probable cause to support the contemporaneously filed Applications, it does not include each and every fact known to me or to other investigators.

4. Based on my training and experience and the facts as set forth in this Affidavit, there is probable cause to believe that evidence, fruits, and instrumentalities of the violation of Title 18, U.S.C. §§ 1029(a)(3) and (b) (possession of 15 or more access devices, and conspiracy to commit the same), 1029(a)(2) and (b) (use/trafficking in unauthorized access devices, and conspiracy to commit the same), 1343 (wire fraud), and 1349 (wire fraud conspiracy). Your Affiant will set forth probable cause to search the person, premises, and vehicle described in Attachment A1 and A2 for evidence, instrumentalities, contraband or fruits of these crimes further described in Attachment B.

STATUTORY AUTHORITY

5. Title 18 U.S.C. § 1029(a)(3) prohibits "knowingly and with intent to defraud possess[ing] fifteen or more devices which are counterfeit or unauthorized access devices." Title 18 U.S.C. § 1029(a)(2) prohibits "knowingly and with intent to defraud traffic[ing] in or use[ing] one or more unauthorized access devices during any one-year period, and by such conduct obtain[ing] anything of value aggregating $1,000 or more during that period." An "access device" is "any card, plate, code, account number, electronic serial number, mobile identification number, personal identification number . . . or other means of account access that can be used, alone or in conjunction with another access device, to obtain money, goods, services, or any other thing of value, or that can be used to initiate a transfer of funds (other than a transfer originated solely by paper instrument)." Title 18 U.S.C. § 1029(e)(1). Title 18 U.S.C. § 1029(b) prohibits attempts and conspiracies of the offenses under 1029(a).

6. "Whoever, having devised or intending to devise any scheme or artifice to defraud, or for obtaining money or property by means of false or fraudulent pretenses, representations, or promises, transmits or causes to be transmitted by means of wire, radio, or television communication in interstate or foreign commerce, any writings, signs, signals, pictures, or sounds for the purpose of executing such scheme or artifice" is in violation of Title 18 U.S.C. § 1343. Conspiring to commit wire fraud – that is, to violate 18 U.S.C. § 1343 – is a federal offense in its own right. See 18 U.S.C. § 1349.

CREDIT CARD SKIMMING

7. Credit card skimming or "carding" is the practice of stealing information associated with payment cards, including account numbers and PIN codes. The card information is used for personal gain by cloning the cards for unauthorized use or by selling the card information on online carding forums or dark web marketplaces. Carding forums and marketplaces commonly also sell stolen identity information. The skimmed card information is commonly sold in bulk after a large number of card details have been collected. Card information is then digitally written on the magnetic strip of different cards ("counterfeit" or "cloned" cards). Gift cards and prepaid debit cards are commonly used for this purpose. Items purchased with cloned cards are often sold for cash as a means of laundering the proceeds. Due to the limitation on Electronic Benefit Transfer (EBT) purchases, cloned EBT cards are often used to purchase bulk food items which can be resold for cash.

8. One method of skimming is to use an "overlay" skimmer which is a device placed over top of payment card terminals used in retails stores and is designed to match the look of the payment terminal used at a checkout counter. The overlay includes a PIN pad which captures the customers PIN code. The device stores the card information and PIN codes and transmits via Bluetooth data from cards swiped through the terminal as well as PINs entered on the overlay.

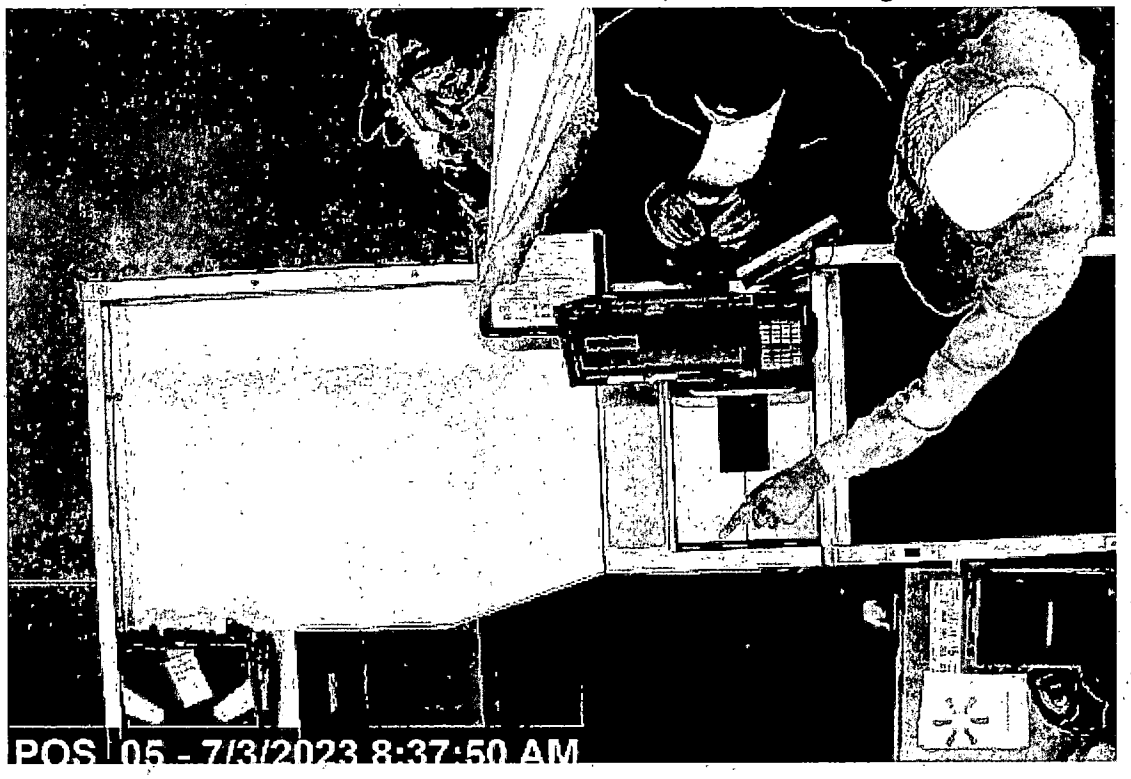
Wal-Mart Credit Card Skimming Investigation

9. In July of 2023, the Buffalo Division of the FBI opened an investigation that was referred to the FBI from the New York State Police (NYSP). Between July 2, 2023, and July 5, 2023, credit card skimming devices were installed at 22 Wal-Mart stores throughout the east coast including 17 stores in New York State (NYS). In most cases the skimming devices were not discovered until a few days after the install date with the latest removal being July 11, 2023.

10. Based on surveillance footage, law enforcement discerned that the scheme works as follows: A group of three individuals install the skimmer. Then, two different individuals return after a few days have passed to collect information with a magnetic activation tag. New York State Intelligence Center has identified four out of the five individuals associated with the skimming devices by sharing obtained video footage of effected Wal-Mart Stores with law enforcement and intelligence analysts who have in depth knowledge of skimmers, specifically the Texas Financial Fusion Center and the South Carolina State Law Enforcement. The four identified individuals are Floarea Linu (Linu), Romario Serban (Serban), Cristian Dunca (Dunca), and Eugina Stoica (Stoica).

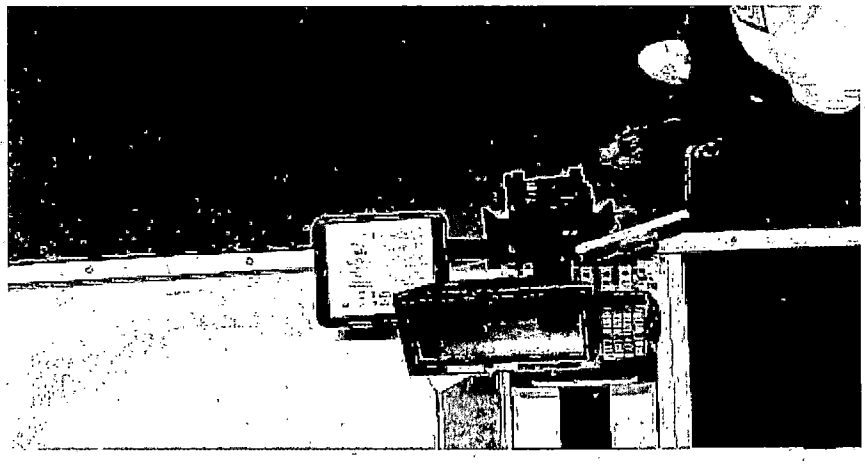
11. Multiple overlay card skimming device were recovered in July 2023 on card readers in Wal-Mart stores located in Watkins Glen, Painted Post, and Elmira, New York (NY). Security video provided by Wal-Mart depicted what appears to be Dunca, Eugina, and an unknown subject (UNSUB) working in a group of three to surreptitiously install the card skimmers throughout Wal-Mart stores. The below still shot from the video footage shows Dunca, Eugina, and UNSUB working together to install the skimming device at a Wal-Mart in Painted Post, NY. Additional footage was reviewed showing the same pattern at various Wal-Mart stores in New York. The individuals are wearing what appears to be the same clothing at each store.

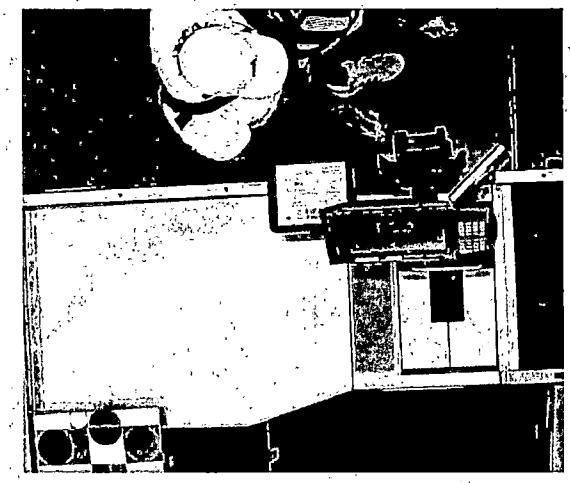
Still shot of skimmer installation from Painted Post, NY video footage:



12. Security video provided by Wal-Mart depicted Serban and Linu returning to the Painted Post Wal-Mart on two separate occasions days after the devices were installed by Dunca, Eugina, and UNSUB. Serban and Linu are then shown working together to surreptitiously retrieve data from the card skimmers using a magnetic activation tag for the skimmer located on the key ring. Additional footage from other Wal-Mart locations shows Serban and Linu repeating the same pattern that took place at the Painted Post, NY Wal-Mart. Serban and Linu have also been linked to the Saratoga Spring, NY and Cobleskill, NY Wal-Mart where they were believed to be seen stealing an iPhones from a display. The individuals are wearing what appears to be the same clothing at each store.

Still shot of data retrieval from Painted Post, NY video footage:

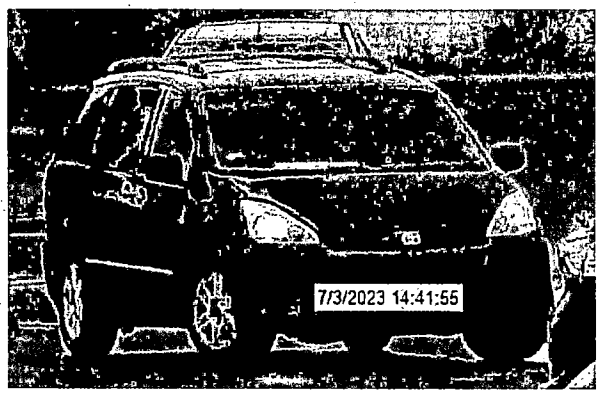


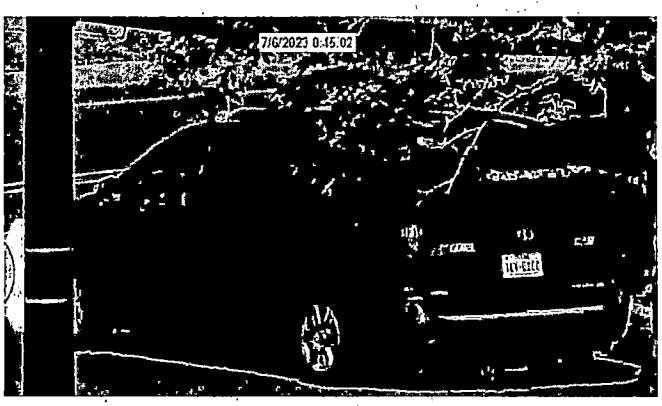


13. Additionally, the video footage provided by Wal-Mart identified three vehicles associated with the subjects. Two vehicles are believed to be in Houston, Texas. A 2005 Toyota Sienna Van bearing Texas Registration TCV6966 (VEHICLE TO BE SEARCHED) was in Pennsylvania at the time of identification and subsequently was stopped and held for evidence by the Pocono Township PD (PTPD). The vehicle has been sealed and secured in evidence in anticipation of a search warrant. NYSP hot listed VEHICLE TO BE SEARCHED'S license plate so that if the license plate was read on a License Plate Reader (LPR) it would alert NYSP and the LPR reader that a stop and hold was put in place for the vehicle associated with the license plate. A PTPD patrol car drove past the VEHICLE TO BE SEARCHED which activated the LPR and notified NYSP that the VEHICLE TO BE SEARCHED'S license plate had a read. NYSP then reached out to the PTPD and explained the VEHICLE TO BE SEARCHED'S connection to the skimming devices.

14. Security video provided by Wal-Mart has placed the VEHICLE TO BE SEARCHED at multiple Wal-Marts throughout the northeast. Linu and Serban have both been associated with the below car, including in the most recent stop on July 17, 2023, by PTPD. PTPD stopped the vehicle after being requested to by NYSP due to its likely connection with skimming events. Once stopped the driver of the vehicle was identified as Serban and his passenger was identified as Linu. Serban was asked for consent to search his person and vehicle to which he granted. A cursory search of the vehicle was performed identifying totes of clothing, a laptop bag containing several iPads and iPhones and a round magnet attached to the vehicle's keys. This round magnet is believed to be the tool used to retrieve data from the skimming devices. The property inside the vehicle and the property on the individuals was consistent to what was seen in surveillance footage and what had been reported stolen at Wal-Mart. The vehicle was then placed in PTPD impound lot and the doors were sealed with evidence tape.

Still shot of VEHICLE TO BE SEARCHED in a Wal-Mart parking lot:





15. The VEHICLE TO BE SEARCHED was previously registered in Georgia (GA) with GA registration CUX4689. LPR identified GA CUX4689 as being in NYS from 6/1-6/4/23 and on 6/4/23, Serban was stopped by NYSP in Verona for a traffic infraction. GA CUX4689 registration was terminated on 06/22/23. On 06/22/23 the VEHICLE TO BE SEARCHED was then re-registered to an Ilja Adi at 2923 Hayes Rd, Apartment 202, Houston, Texas (TX). VEHICLE TO BE SEARCHED was seen back in NY on LPRs in Binghamton on 07/07/23. The day after TX TCV6966 was believed to be at the Watkins Glen, NY Wal-Mart. The VEHICLE TO BE SEARCHED was believed to be seen through surveillance footage on 07/16/23 at a Cobleskill Wal-Mart where an iPhone display was stolen.

16. The 2005 Toyota Sienna Van bearing Texas Registration TCV6966 (VEHICLE TO BE SEARCHED) was in Pennsylvania at the time of identification and subsequently was stopped and held for evidence by the Pocono Township PD (PTPD). The vehicle has been sealed and secured in evidence in anticipation of a search warrant. From a lawful vantage point officers observed a "shoulder bag" identified in the above-photographs, a magnetic activation tag in form of key fab which is commonly used to relay the stolen data from another device, and totes which appear to have stolen items within it, located inside the vehicle.

17. In my training and experience, members of criminal enterprises often maintain multiple mobile phones in order conceal their identities, communications, and criminal activity. Often

these devices are prepaid and do not require identification to purchase or to activate. I also know that members of criminal enterprises often obtain and use fake identification documents which are used to make purchases and conduct financial transactions.

18. In my training and experience, members of criminal enterprises which conduct interstate operations will travel with their phones so they can maintain communication and conduct skimming operations. The location of these devices can be used to identify the location of active skimmers as well as historical victims.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

28. This application seeks permission to search for records that might be found on the in the SUBJECT VEHICLE in whatever form they are found. One form in which the records are likely to be found is data stored on a mobile device (e.g., a phone or tablet) or computer. Thus, the warrant applied for would authorize the seizure of mobile devices/computers and the copying of electronically stored information, all under Rule 41(e)(2)(B).

29. I submit that if a mobile device/computer is found in the SUBJECT VEHICLE there is probable cause to believe those records referenced above will be stored on that mobile device/computer. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

30. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the devices were used, the purpose of

its use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the devices because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

b. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

c. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

31. I also know that during the search of a premises, vehicle, or person it is not always possible to search mobile devices/computers for data for a number of reasons, including the following:

a. Searching mobile devices/computers is a technical process that requires specific expertise and specialized equipment. If the device is locked and the password is unknown, the process is further complicated and may require specialized techniques.

b. The volume of data stored on mobile devices/computers will typically be so large that it will be highly impractical to search for data during the execution of a physical search; and

c. Mobile device/computer users can attempt to conceal data within unassuming or locked application. A substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

32. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing mobile devices/computers that reasonably appear to contain some or all of the evidence described in the warrant and would authorize a later review of the data contained therein.

CONCLUSION

33. I submit that this Affidavit supports probable for a warrant to search the vehicle described in Attachment A, and seize the items described in Attachment B.

Respectfully submitted,

/s/ F. Xavier Deluke
F. Xavier Deluke
Special Agent
Federal Bureau of Investigation

Sworn to and subscribed before me
by reliable elctronic means this
20th day of September, 2023.

Joseph F. Saporito, Jr.
JOSEPH F. SAPORITO, JR.
UNITED STATES MAGISTRATE JUDGE

This Affidavit was reviewed by AUSA Brian J GALLAGHER

In accordance with Rule 4.1(b)(2)(A), the Affiant attested under oath to the contents of this Affidavit, which was submitted to me by reliable electronic means, on the 12th of September 2023, at 9:00 a.m.

ATTACHMENT A

DESCRIPTION OF VEHICLE TO BE SEARCHED

A 2005 Toyota Sienna, blue in color having Texas license plate number TCV6966 and vehicle identification number 5TDZA22C25S234412 which was seized by law enforcement on July 17, 2023, in conjunction with a traffic stop. The vehicle is currently located at the Pocono Township Police Department. The van is pictured below:

ATTACHMENT B

Items to be Searched for and Seized

All items and records that relate to violations of Title 18 U.S.C. §§ 1029(a)(3), 1029(a)(2), and 1029(b) (access device fraud and conspiracy to the commit the same) and 18 U.S.C. §§ 1343 and 1349 (wire fraud and conspiracy to commit the same) including, but not limited to:

1. Card skimming equipment, including card readers/writers.

2. Any and all items and processes that would tend to identify occupants of the vehicle, routes that the vehicle had taken, communication between parties associated with the vehicle, in any form, including electronic, and forensic (fingerprints, DNA, ect.) evidence.

3. Cards with magnetic strips, including gift cards and pre-paid cards.

4. Proceeds of card skimming fraud such as bulks cash and bulk goods.

5. Clothing or accessories depicted in surveillance video footage of individuals installing skimming devices or conducting fraudulent EBT transactions from stores in the Northeast in the last twelve months.

6. Mobile devices (e.g., phones and tablets) and computers that could be used as a means to commit the violations described above, and on which the things described in this warrant could be stored.

7. Records, information, and items relating to violations of the statutes described above in the form of:

a. Records and information related to the receipt, possession, or trafficking of EBT card numbers, including credentials to decrypt data on skimmers;

b. Records and information related to the proceeds of EBT card number theft and laundering thereof;

c. Records and information related to individuals engaged in the receipt, possession, or trafficking of EBT card numbers including their identity and location; and

d. Records, information, and items related to the occupancy or ownership of the subjects residence including utility and telephone bills, mail envelopes, or addressed correspondence.

8. For any mobile device or computer whose seizure is otherwise authorized by this warrant:

a. evidence of who used, owned, or controlled the mobile device at the time the things described in this warrant were created, edited, deleted, viewed, or otherwise interacted with;

b. evidence of how and when the mobile device was used to create, edit, delete, view, or otherwise interact with or engage in the things described in this warrant;

c. passwords, encryption keys, and other access devices that may be necessary to access the mobile device;

d. evidence of software that would allow others to control the mobile device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

e. evidence of programs (and associated data) that are designed to eliminate data from the mobile device;

9. During the course of the search, photographs of the location to be searched may be taken to record the condition thereof and/or the location of items therein.

If the government identifies seized materials, that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e., communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (e.g., the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team.